ARMY REGULATION
No. 381-12

HEADQUARTERS
DEPARTMENT OF THE ARMY
WASHINGTON, DC, *1 July 1981*

MILITARY INTELLIGENCE

SUBVERSION AND ESPIONAGE DIRECTED AGAINST US ARMY (SHORT TITLE: SAEDA)

Effective 1 August 1981

This regulation requires DA personnel to report at once any incidents or situations that have to do with subversion and espionage directed against or affecting the US Army and national security. It describes the espionage threat by foreign intelligence services and provides guidance, establishes procedures, and prescribes responsibilities for countering the threat.

Local supplementation of this regulation is prohibited, except upon approval of the Assistant Chief of Staff for Intelligence. Requests for exception with justification will be sent through command channels to HQDA (DAMI-CIC), WASH DC 20310.

Interim changes to this regulation are not official unless they are authenticated by The Adjutant General. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

*This regulation supersedes AR 381-12, 18 October 1974.

1. Purpose. This regulation sets forth responsibilities, guidance, and procedures for the prompt recognition and reporting of incidents of attempted criminal subversion, sabotage, international terrorism, espionage directed against the US Army and its personnel, or deliberate compromises of classified information. It also provides for the training of Army personnel in such matters.

2. Applicability. This regulation applies to all DA personnel (military and civilian) and members of the Army National Guard and the US Army Reserve.

3. Explanation of terms. See appendix A.

4. General. *a.* The US Army has installations and personnel located worldwide. It is a prime and easily accessible target for foreign intelligence services (friendly and hostile) and sympathizers of foreign governments. It is vulnerable to subversion and espionage in the continental United States (CONUS) and outside CONUS. By themselves, the defensive security measures designed to prevent sabotage of US Army facilities and materiel and the compromise of classified information are not enough. DA personnel (military, civilian, and dependents) are the key to an effective counterintelligence (CI) program. Dependents should be instructed to tell their sponsors of any incidents reportable under this regulation.

b. The methods used by foreign intelligence services and other disruptive elements to get information from, or to enlist the services of, DA personnel are many and varied. They range from a seemingly accidental or spontaneous meeting to threats of exposure for a moral indiscretion. A common trend after a friendship has developed is for a member of a foreign intelligence service to request unclassified documents or information which is later followed by requests or demands for classified information.

c. A positive SAEDA program must be established by Army commanders at all levels to indoctrinate all DA personnel on the methods used to subvert or entrap them. This is crucial for those whose positions, duties, or access make them attractive targets of foreign intelligence services.

5. Responsibilities. *a. Assistant Chief of Staff for Intelligence (ACSI).* The ACSI will—

(1) Exercise DA Staff responsibility for the Army's SAEDA program.

(2) Monitor all aspects of the SAEDA program to determine program effectiveness.

(3) Establish policy and issue regulatory guidance for processing and investigating reported SAEDA incidents and situations.

(4) Apprise higher authorities of significant SAEDA incidents and situations.

(5) Advise major Army commanders of information developed by the US intelligence community that requires special SAEDA briefings for selected Army personnel.

b. Commanding General (CG), US Army Intelligence and Security Command (INSCOM). The CG INSCOM will—

(1) Operate the SAEDA program for the ACSI.

(2) Represent the ACSI in matters pertaining to SAEDA reporting and investigations worldwide.

(3) Control or monitor for the ACSI all investigations or other actions resulting from any SAEDA reporting worldwide.

(4) Provide appropriate information to commanders regarding SAEDA incidents and situations involving their personnel.

(5) Support the SAEDA program by maintaining a data base of sufficient scope to portray the program's status, effectiveness, and efficiency and its impact on the overall CI and security posture of the Army. The data base will contain the following:

(*a*) Total number of DA personnel within each command.

(*b*) Total number of DA personnel briefed on SAEDA within each command during the fiscal year.

(*c*) Total number of briefings, within each major Army command (MACOM) and on a fiscal year basis, conducted by personnel assigned to—

1. INSCOM units.

2. Tactical MI units.

3. Offices of Security Officers or Managers, and all others.

(6) Report SAEDA data base statistics annually to HQDA(DAMI-CIC) not later than 45 days following the end of the fiscal year, RCS CSGID-156.

(7) Prepare and present SAEDA and special SAEDA briefings as required.

c. MACOM commanders. All MACOM commanders will—

(1) Establish an annual SAEDA training program which will reach all levels of subordinate units and supported commands.

(2) Insure that SAEDA training is incorporated into command training programs conducted under AR 350-1 and is compatible with requirements of this regulation.

(3) Monitor the SAEDA program to insure that annual SAEDA briefings are given to all personnel.

(4) Maintain and submit statistical data to support the INSCOM data base. Information for the data base as prescribed in *b*(5)(*a*), (*b*), and (*c*) above will be sent to CDR USAINSCOM, ATTN: IAOPS-OP-OC, Fort Meade MD 20755, not later than 30 days following the end of the fiscal year.

d. Commanders, tactical MI units. Commanders of these units, in coordination with supported commanders and INSCOM units, will—

(1) Prepare and present annual SAEDA briefings, and when requested by supported commanders, special SAEDA briefings. Advice, guidance, assistance, and briefing materials can be obtained from INSCOM.

(2) Maintain and submit statistical data to supported commands to support the INSCOM data base (para *b*(5) and *c*(4) above).

(3) Insure that SAEDA reports (para 9) are forwarded promptly to INSCOM through intelligence channels and that no other action is taken without appropriate control office approval.

6. SAEDA training. *a.* DA personnel will receive a SAEDA briefing each year. These briefings will be presented by qualified CI personnel to the maximum extent possible, as shown below:

(1) Briefings at echelons above corps will be presented by INSCOM.

(2) Briefings in tactical units at corps level and below will be presented by the supporting tactical MI unit having a CI capability.

(3) When distance precludes or INSCOM or tactical MI unit personnel are not available, SAEDA briefings will be presented by unit security officers or managers. Briefing materials provided by INSCOM or the tactical MI unit will be used, if appropriate.

b. SAEDA briefings will be prepared specifically for the particular audience and geographic area in which they are given and will be classified accordingly. As a minimum, briefings will contain instruction on the following:

(1) Methods and techniques used by foreign intelligence services to obtain information on Army facilities, activities, personnel, or materiel.

(2) The fact that foreign intelligence services consider DA personnel as potential sources for US defense information.

(3) The nature of the international terrorist threat, the vulnerabilities of DA personnel and their dependents to international terrorist acts, and the defense measures that can be used to thwart such acts.

(4) Reporting procedures (paras 8 and 9).

7. SAEDA special briefings. *a.* Certain personnel are especially vulnerable to hostile approach by virtue of their position, travel, duties, or activities. These include, but are not limited to, those having access to compartmented information or special access programs or occupying positions of special interest to foreign intelligence services. These include senior DA executives, research and development specialists, and scientific, technical, intelligence, and CI personnel.

b. Security managers will insure that personnel receive special briefings, as prescribed in paragraph 6*a* and *b*, when they—

(1) Are scheduled to travel on leave or TDY to or through areas of special concern (app B).

(2) Are scheduled to attend international scientific, technical, engineering or other professional meetings in CONUS or outside CONUS in which representatives of Communist-controlled countries are likely to participate or be in attendance.

(3) Have close relatives residing in an area of special concern. Special briefings for DA personnel in this category generally will be given only once. However, they may be repeated for emphasis if the person assumes more sensitive duties, is reassigned to a more vulnerable location, or for other similar reasons.

(4) Are scheduled to travel to an area where there is reason to believe that a hostage situation exists, or may develop, that could result in exploitation of such persons by a foreign intelligence service or international terrorist organization.

c. Special SAEDA briefings will be tailored to the particular risk involved, to include inherent hazards and vulnerabilities. They also should include elements of the annual briefings, as appropriate, with emphasis on reporting responsibilities.

8. Incidents and situations to be reported. Reporting of incidents and situations described in this paragraph is mandatory. Reports will comply with the procedures given in paragraph 9. Failure to report such incidents or situations constitutes a violation of this regulation and may provide the basis for disciplinary action under the Uniform Code of Military Justice (UCMJ) or other authority

as appropriate. Incidents and situations are as follows:

a. Attempts by unauthorized persons to obtain classified or unclassified information concerning US Army facilities, activities, personnel, or materiel through questioning, elicitation, trickery, bribery, threats, or coercion, either through direct or indirect personal contacts or correspondence.

b. Attempts by unauthorized persons to obtain classified or unclassified information through photographs, observation, collection of documents or materiel, or by any other means.

c. Attempts by persons with known, suspected, or possible foreign intelligence backgrounds, associations, or activities to establish any type of friendship or social or business relationship, or to place DA personnel under obligation through special treatment, favors, gifts, money, or other means.

d. All incidents where DA personnel, or their dependents, traveling to or through foreign areas of special concern (app B) are—

(1) Subjected to questions regarding their duties.

(2) Requested to provide military information.

(3) Threatened, coerced, or pressured in any way to cooperate with a foreign intelligence service.

e. Incidents of known, suspected, or possible espionage which resulted in, may have resulted in, or in the future may result in the compromise of classified documents, information, or materiel.

f. Other acts of deliberate compromise committed, attempted, or contemplated by DA personnel with the intention of conveying classified documents, information, or materiel to any unauthorized person.

g. Nonofficial contacts by DA personnel with—

(1) Persons whom they know or suspect to be members of a foreign intelligence or security service.

(2) Foreign military or police organizations.

(3) Any officials of countries listed in appendix B.

h. Official contacts with persons described in *g* above when such persons—

(1) Show undue knowledge or curiosity about the DA member.

(2) Attempt to obtain classified or unclassified information from the DA member.

(3) Attempt to establish any type of friendship or social or business relationship with the DA member which is outside the range of normal official duties.

i. Information concerning international terrorist plans and activities posing a direct threat to facilities, activities, personnel, or materiel.

j. Known or suspected acts or plots to harm or destroy defense property by sabotage.

9. Reports. *a. Reporting procedures.*

(1) All DA personnel who have been involved in or have knowledge of a SAEDA incident or situation will report all facts immediately to the nearest INSCOM or tactical MI office. If these are not readily available, SAEDA incidents or situations will be reported to the unit commander, or unit or organization security officer/manager or intelligence officer. These persons will insure that the report is transmitted as soon as possible, but in all cases with 24 hours to the nearest supporting INSCOM or tactical MI office. Knowledge of the SAEDA incident or situation will be limited to as few persons as possible and only those who have a need to know.

(2) DA personnel assigned to Supreme Headquarters Allied Powers Europe and other elements of Allied Command Europe who have been involved in or who have knowledge of a SAEDA incident or situation will report all facts immediately to the nearest office of the 650th Military Intelligence Group.

(3) If the DA member is located or traveling outside the United States in an area where there is no INSCOM or tactical MI unit, and the SAEDA incident or situation is important enough to require immediate action, a SAEDA report will be submitted to the nearest US military authority, intelligence or security officer, US Defense Attache Office, or US Consulate Security Officer. If the SAEDA information is not of an urgent nature, a SAEDA report will be submitted to the nearest supporting INSCOM or tactical MI unit upon completion of travel.

(4) INSCOM and tactical MI units receiving a SAEDA report will—

(*a*) Obtain complete details and submit a report by priority or immediate electrical message as urgency dictates to the addressees and in the format shown in appendix C.

(*b*) Take no further action and make no further dissemination unless directed by, coordinated with, or concurred in by the appropriate

control office. See paragraph A-4, appendix A.

(c) Inform DA personnel making a SAEDA report that they may be contacted by a representative of INSCOM and they are not to reveal the existence or nature of the incident or situation to anyone else.

(5) If other DA organizations, offices, or agencies are contacted by DA personnel seeking to submit a SAEDA report, they will be guided by the above procedures.

b. Communications procedures.

(1) All initial SAEDA reports will be submitted electrically by INSCOM and tactical MI units in the format in appendix C. All reports receive limited distribution (LIMDIS).

(2) The Defense Special Security Communications System (DSSCS) will be used when possible. The DSSCS and the terms SSO message, SSO service and SSO channels all mean the same thing. When SSO service is not available, SAEDA reports will be submitted electrically via the General Service message system.

c. Security classification. All SAEDA reports will be classified according to the SAEDA Classification Guide in appendix D.

d. Investigative reports. SAEDA reports will be forwarded through CI channels to CDR, USAINSCOM, ATTN: Commander, Special Operations Detachment, Fort Meade MD 20755.

e. Information requirements control. SAEDA reports submitted under this regulation are exempt from information requirements control under paragraph 7-2r, AR 335-15.

10. Non-US citizens. The use of this regulation for non-US citizen employees and contractors of DA installations and commands located in foreign countries will be according to the Status of Forces Agreement or treaty between the US and host country governments.

APPENDIX A

EXPLANATION OF TERMS

A-1. Agent of a foreign power. *a.* Any person, other than a United States person, who—

(1) Acts in the United States as an officer or employee of a foreign power or as a member of a group engaged in international terrorism or activities in preparation therefore.

(2) Acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicates that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities.

b. Any person who—

(1) Knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power which activities involve or may involve a violation of the criminal statutes of the United States.

(2) Pursuant to the direction of an intelligence service or network of a foreign power knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities invclve or are about to involve a violation of the criminal statutes of the United States.

(3) Knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore, for or on behalf of a foreign power.

(4) Knowingly aids or abets any person in the conduct of activities described in subparagraphs (*a*) and (*b*) or knowingly conspires with any person to engage in activities described in subparagraphs (*a*) and (*b*).

A-2. Clandestine intelligence activity. An activity conducted for intelligence purposes or for the purpose of affecting political or governmental processes by or on behalf of a foreign power in a manner designed to conceal from the US Government the nature or fact of such activity or the role of such foreign power, and any activity conducted in support of such activity.

A-3. Classified defense information. Official information which requires protection in the interest of national defense and is classified TOP SECRET, SECRET, or CONFIDENTIAL according to AR 380-5.

A-4. Control Office. The office responsible for directing and controlling SAEDA investigations and operations. The following control offices are responsible for all Army SAEDA investigations and operations within their geographic areas for CI investigative responsibilities: (1) Deputy Chief of Staff for Intelligence (DSCI) USAREUR for the CINCUSAREUR area of responsibility; (2) Assistant Chief of Staff, G-2 (ACofS, G-2), Eighth USA for the CDR Eighth US Army area of responsibility; and (3) Commander, Special Operations Detachment, INSCOM, for all other areas.

A-5. Contact(s). Any form of meeting, association, or communication with any person of the concerned areas listed in appendix B, even if no official information is discussed. This includes any contact in person, or by radio, telephone, letter, or any other form of communication, whether it is for social, private, or any other reason. It also means any visit to any embassy, consulate, trade or press office, or other official building or office of a Communist country, whether the visit is for private or official reasons.

A-6. Counterintelligence. Information gathered and activities conducted to protect against espionage and other clandestine intelligence activities, sabotage, international terrorist activities, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, but not including personnel, physical,

document, or communications security programs.

A-7. Counterintelligence investigation. Inquiries and other activities undertaken to determine whether a particular US person is acting for, or on behalf of, a foreign power for purposes of conducting espionage and other clandestine intelligence activities, sabotage, and international terrorist activities.

A-8. Criminal subversion. Criminal subversion is defined in Section 2387, Title 18, United States Code. Its elements generally are actively encouraging military or civilian personnel of the Department of Defense to violate laws, disobey lawful orders or regulations, or disrupt military activities, with the willful intent thereby to interfere with, or impair the loyalty, morale, or discipline of, the military forces of the United States.

A-9. DA personnel. Persons employed by the Department of the Army. It includes both military and civilian employees.

A-10. Deliberate compromise of classified information. There are two types of deliberate compromise applicable to this regulation. They are instances where classified defense information is compromised or possibly compromised as a result of—

a. Espionage or suspected espionage activity.

b. Willful disclosure to an unauthorized person.

A-11. Espionage. The elements of espionage as set forth in section 792-798, Title 18, United States Code are generally as follows:

a. Espionage is the act of obtaining, delivering, transmitting communicating, or receiving information in respect to the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The offense of espionage applies in time of war or peace.

b. The statute makes an offense the gathering of national defense information with the requisite intent or belief by going upon, entering, flying over, or obtaining access by any means to any installation or place used by the United States in connection with national defense. The method of gathering information is immaterial.

c. Whoever lawfully or unlawfully has possession of, access to, control over, or is entrusted with, information dealing with national defense, which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, and willfully communicates or transmits, or attempts to communicate or transmit such information to any person not entitled to receive it is guilty of espionage under the statute.

d. The statute on espionage also provides that anyone entrusted with, or having lawful possession or control of information pertaining to national defense, who through gross negligence permits same to be lost, stolen, abstracted, destroyed, removed from its proper place of custody, or delivered to anyone in violation of this trust, is guilty of violation of the Espionage Act.

e. If two or more person enter into a conspiracy to commit and one of them commits an overt act in furtherance of such conspiracy, all members of the conspiracy may be punished for violation of the Espionage Act. The same principle regarding conspiracy also applies to the complaint case categories of sabotage and sedition.

A-12. Foreign intelligence. Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons. This does not include CI except for information on international terrorist activities.

A-13. Foreign power. Any foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign based terrorist group, or any organization composed, in major part, of any such entity or entities.

A-14. Foreign Intelligence Service. An organization of a foreign government which engages in intelligence activities.

A-15. Intelligence. Foreign intelligence and CI (see paras A-6 and A-12).

A-16. Intelligence method. Any process, mode of analysis, means of gathering data, or processing system or equipment used to produce intelligence.

A-17. Intelligence source. A person or technical means that provides intelligence.

A-18. International terrorist activities. Any activity or activities which—

a. Involve killing, causing serious bodily harm, kidnapping, or violent destruction of property, or an attempt or credible threat to commit such acts; and

b. Appear intended to endanger a protectee of the Secret Service or the Department of State or to further political, social, or economic goals by intimidating or coercing a civilian population or any segment thereof, influencing the policy of a government or international organization by intimidation or coercion, or obtaining widespread publicity for a group or its causes; and

c. Transcend national boundaries in terms of the—

(1) Means by which it is accomplished.

(2) Civilian population, government, or international organization it appears intended to coerce or intimidate.

(3) Locale in which its perpetrators operate or seek asylum.

A-19. Sabotage. Any activity that involves a violation of chapter 105 of Title 18, United States Code, or that would involve such a violation if committed against the United States.

APPENDIX B

GEOGRAPHICAL AREAS OF SPECIAL CONCERN

Afghanistan
Albania
Angola
Bulgaria
Cambodia
China (People's Republic of)
Chinmen (Quemoy), Matsu, and other islands offshore from mainland China held by the Government of Taiwan
Cuba (except US Naval Base, Guantanamo)
Czechoslovakia
Ethiopia
German Democratic Republic (East Germany)
Hungary
Iran
Iraq
Laos
Lebanon
Libyan Arab Republic
North Korea (and adjacent demilitarized zone)
Outer Mongolia (Mongolian People's Republic)
Poland
People's Democratic Republic of Yemen
Romania
Soviet Sector of Berlin
Syria
Union of Soviet Socialist Republics (USSR)
Vietnam
Yugoslavia

APPENDIX C

SAEDA MESSAGE FORMAT

C–1 Guidance for preparing SAEDA messages. *a.* The SAEDA electrical report will comply with the format shown in paragraph C–3. It will be classified according to appendix D. All paragraph and subparagraph titles will be included in the transmitted report.

b. SAEDA investigative reports will be prepared in accordance with DA Pamphlet 381-20 (Counterintelligence Investigative and Reporting Procedures) and INSCOM directives and instructions.

c. If a full report will cause undue delay, submit an interim report with information that is available.

d. SAEDA messages will be caveated with either "Night Action Required" or "Deliver During First Duty Hours."

C–2. Message addressees. All SAEDA electrical messages will be addressed as follows:

a. SSO messages.

FROM: SSO (Station Designator)
TO: SSO MEADE
(Other Appropriate SSO Station)
INFO: SSO DA/DAMI-CIC//
QQQQ
DELIVERY INSTRUCTIONS: (Night Action Required) or (Deliver During First Duty Hours)

CLASSIFICATION LIMDIS (Station Designator _____ TOPIC): (If the SSO Station is not authorized to use its own message numbering system on the next line use the following:)

CITE: (Office Designation) (No. of Message) TOPIC: (Example: CITE XXXX 0011 TOPIC)

FROM: (Person Sending Message) (Office/Area Designation) (Example: COL XXXX, Chief, XXXX, XXXX, USAREUR)

TO: COL _____, CDR, SP OPS DET, INSCOM, FT MEADE MD
(Other Appropriate SSO Stations)

INFO: COL _____, DIR, CI, OACSI, DA (Pass to Mr. _____, SOD LNO) SUBJECT: SAEDA ( )

b. General Service messages.

FROM: (HQ Sending Message//Office Designation//
TO: CDRSPECOPNS DET USAINSCOM FT MEADE MD//IASO-CO//
(Other Appropriate Addressees)
INFO: HQDA WASH DC//DAMI-CIC//
(CLASSIFICATION)LIMDIS
DELIVERY INSTRUCTIONS: (Night Action required) or (Deliver During First Duty Hour)

SUBJECT: SAEDA ( )

c. Additional information addressees. Such addressees may be added only as specified authorized by INSCOM directives and instructions.

C-3. Message format. The body of all SAEDA electrical messages will be as follows:

CONFIDENTIAL LIMDIS TOPIC
SUBJECT: SAEDA ( )
A. (References)

1. ( ) Date of incident.
2. ( ) Location of incident.
3. ( ) Persons involved (See Note 1.)
   a. ( ) Source(s). (See Note 2.)
   b. ( ) Witness(es). (See Note 2.)
   c. ( ) Others knowledgeable. (See Note 3.)
   d. ( ) Suspect(s). (See Note 2.)
4. ( ) Narrative. (See Note 4.)
5. ( ) Actions taken.
6. ( ) Comments. (See Note 5.)

Note 1. Provide the following information for each person(s) listed by name (last name, first name, and middle initial); D&POB, SSN; organization to which assigned, to include unit in which incident occurred; duty position; ETS; DEROS; security clearances; special access; and date of last SAEDA briefing.

Note 2. If more than one source, each should be listed as Source 1, Source 2, and so forth. The same procedure applies if there is more than one witness or suspect. If identification data are not known for witness(es) or suspect(s), list available physical description.

Note 3. Individuals knowledgeable of the incident should be identified in the same manner as persons involved.

Note 4. List complete factual description of incident as reported by source(s), starting with details concerning how the source(s) came to the attention of the INSCOM or tactical MI unit reporting the SAEDA incident.

Note 5. Submit any comments, remarks, or recommendations pertinent to the incident, source(s), or suspect(s).

APPENDIX D

SAEDA CLASSIFICATION GUIDE

D-1. Security classification. SAEDA reports will be classified CONFIDENTIAL unless, in unusual circumstances, the originator of the report decides that its content warrants a higher classification (see para D-5c).

D-2. Authority. SAEDA reports classified CONFIDENTIAL will cite this regulation as the authority for classification.

D-3. Duration of classification. SAEDA reports classified CONFIDENTIAL solely because of the requirements of this regulation will be marked for declassification review 10 years from the date of the report. The reason for extension of classification beyond 6 years is as stated in paragraph 2-301c(3), AR 380-5. This extension has been authorized by the ACSI, HQDA.

D-4. Marking. Electrically transmitted SAEDA reports classified solely because of the requirements of this regulation will contain the following statement as the last line of the message:

"CLASS BY AR 381-12; REVW (insert appropriate date)"

D-5. Special circumstances. Special circumstances may require classification of SAEDA reports at a level higher than CONFIDENTIAL or for a longer period than indicated in paragraph D-3. In such cases, the following instructions will apply:

a. Reports containing SECRET or TOP SECRET information will be marked with the highest classification of information they contain.

(1) The declassification instructions will specify the date established for declassification or review of the SECRET or TOP SECRET information, or a review date 10 years from the date of the report, whichever is later.

Examples:

1. A report dated 10 Jun 79 contains SECRET data which is to be declassified on 31 Dec 93. Mark this report for declassification on 31 Dec 93.

2. A report dated 10 Jun 79 contains SECRET data which is to be declassified 31 Dec 91. Mark this report for review 10 Jun 89.

(2) The last line of the message will read as follows:

"CLASS BY MULTIPLE SOURCES; REVW (insert appropriate date)"

b. If it is necessary to include information in the report which has been classified CONFIDENTIAL for reasons and by authority other than this regulation, the declassification instructions for the report will be determined as prescribed in *a* above.

c. If the originator of a SAEDA report has reason to believe that information in the report, due to its potential for damage to the national security, warrants a classification higher than CONFIDENTIAL, but the information has not otherwise been classified, a tentative classification at a higher level may be applied. The commander, Special Operations Detachment, INSCOM, will obtain an evaluation of the material according to paragraph 2-600, AR 380-5, and will notify all recipients of the report of the results of the evaluation. The originator of the report

will mark it with the security classification he or she believes appropriate. The last line of the message will read as follows:

"TENTATIVE CLASSIFICATION: PARA D-5c, APP D, AR 381-12."

d. Each paragraph and subparagraph of the record will be marked with the security classification of the information it contains, but in no case lower than CONFIDENTIAL.

The proponent agency of this regulation is the Office of the Assistance Chief of Staff for Intelligence. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) direct to HQDA(DAMI-CIC), WASH DC 20310.

By Order of the Secretary of the Army:

E. C. MEYER
General, United States Army
Chief of Staff

Official:

ROBERT M. JOYCE
Brigadier General, United States Army
The Adjutant General

DISTRIBUTION:
Activy Army, ARNG, USAR: To be distributed in accordance with DA Form 12-9A requirements for AR, Military Intelligence—A

• U.S. GOVERNMENT PRINTING OFFICE: 1983-0-381-663/1029